Evaluation Warning: The document was created with Spire.Doc for Python.

**破解侠（ 0.0.5版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 破解侠 |
| 版本 | 0.0.5 |
| 包名 | hgvf.com |
| 域名线索 | 12条 |
| URL线索 | 9条 |
| APP图标 |  |
| 分析日期 | 2025年6月7日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | o\_1in0dk9701q1svffgaajg1isa9.apk |
| 文件大小 | 44.61MB |
| MD5值 | 1111cfbe8e1e3812ac61ff7458fcf376 |
| SHA1值 | 9de8b7ad0cad7703afecf1c881d365e2d7fe0371 |
| SHA256值 | 2aca6ef8abe0c5f51b115eb14661bc4cabb138f2626c54655ab755aa5321a691 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 破解侠 |
| 包名 | hgvf.com |
| 主活动Activity | com.uzmap.pkg.LauncherUI |
| 安卓版本名称 | 0.0.5 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| xmlpull.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| iuap-yonbuilder-mamservice.yyuap.com | IP: 59.110.247.93  所属国家: China  地区: Beijing  城市: Beijing |
| d.app3c.cn | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| as.app3c.com | 没有服务器地理信息. |
| p.app3c.cn | 没有服务器地理信息. |
| s.app3c.com | 没有服务器地理信息. |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.ccil.org | IP: 142.251.211.243  所属国家: United States of America  地区: California  城市: Mountain View |
| ops.fun.mipm | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | com/apicloud/third/gif/GifTextView.java |
| http://xmlpull.org/v1/doc/features.html | com/deepe/c/c/a/a/n.java |
| http://xml.org/sax/features/external-general-entities | com/deepe/c/c/a/a/n.java |
| http://xml.org/sax/features/external-parameter-entities | com/deepe/c/c/a/a/n.java |
| http://xml.org/sax/properties/lexical-handler | com/deepe/c/c/a/a/n.java |
| http://www.ccil.org/ | com/deepe/c/i/s.java |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | com/deepe/c/l/a.java |
| http://ops.fun.mipm/sync | com/uzmap/pkg/uzcore/e.java |
| http://ops.fun.mipm/sync | com/uzmap/pkg/openapi/SuperWebview.java |
| https://iuap-yonbuilder-mamservice.yyuap.com/iuap-yonbuilder-mobile/v2 | compile/Properties.java |
| https://d.app3c.cn | compile/Properties.java |
| https://s.app3c.com | compile/Properties.java |
| https://p.app3c.cn | compile/Properties.java |
| https://as.app3c.com | compile/Properties.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| x@j.9υ\_1 | 摸瓜V2引擎 |
| r@uh.kx | 摸瓜V2引擎 |
| i@c㦭va.agtxh | 摸瓜V2引擎 |
| de@ˮba.ٯ\_8 | 摸瓜V2引擎 |
| oy@p.ytz | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/deepe/c/c/a/a/o.java |
| 17179869184 | com/deepe/c/c/a/a/j.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-06 14:54:51+00:00 有效期至: 2125-02-10 14:54:51+00:00 发行人: C=zh, ST=Beijing, L=Beijing, O=test, OU=test, CN=www.ctbri.com 序列号: 0x98ba00e 哈希算法: sha1 md5值: c0f295d6687aceaac389eb031c90acef sha1值: b9d764be1645548d8a64917b0f4d280dd7014461 sha256值: b0145ad8f4ca94a59d2499800b30a7b1a919ea7c50b685036689c6d9a213dd2f sha512值: c14a3c815ab7437f766165986c7d357d8b99532944e2d84b96ec657f3c98eb3548d4984c1c90e9f51fb6d7fa6b4a55c763c27a106e8ac15568582e9085ce4a1f 公钥算法: rsa 密钥长度: 1024 指纹: 670258e1e28a3c9405e15484d89e4e1282dc99230bfe34dc96cc2c3e22cb323a**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| android.permission.WRITE\_EXTERNAL\_STORAGE | 危险 | 读取/修改/删除外部存储内容 | 允许应用程序写入外部存储 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_WIFI\_STATE | 正常 | 查看Wi-Fi状态 | 允许应用程序查看有关 Wi-Fi 状态的信息 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.READ\_EXTERNAL\_STORAGE | 危险 | 读取外部存储器内容 | 允许应用程序从外部存储读取 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**